Risk and performance:

Embedding risk management

Think Ahead

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants, offering business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management.

ACCA supports its **208,000** members and **503,000** students in **179** countries, helping them to develop successful careers in accounting and business, with the skills required by employers. ACCA works through a network of **104** offices and centres and more than **7,300** Approved Employers worldwide, who provide high standards of employee learning and development. Through its public interest remit, ACCA promotes appropriate regulation of accounting and conducts relevant research to ensure accountancy continues to grow in reputation and influence.

ACCA is currently introducing major innovations to its flagship qualification to ensure its members and future members continue to be the most valued, up to date and sought-after accountancy professionals globally.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability.

More information is here: www.accaglobal.com

May 2019

Risk and performance:
Embedding risk management

Dr Simon Ashby Vlerick Business School, Belgium

Dr Cormac Bryce City, University of London

Dr Patrick Ring Glasgow Caledonian University

About this report

Ensuring effective risk management in any organisation is essential. This report takes a close examination of the practices organisations are adopting to embed risk management practices across the organisation. Using an in depth case study approach, it explores how businesses can overcome the common challenges presented in implementing effective risk management processes and suggests good practices for aligning these to the delivery of strategic goals.

Foreword

Jamie Lyon
Director of Professional Insights
ACCA

In an increasingly competitive and challenging environment, the effective management of risk is fundamental to an organisation' success. In 2018 ACCA undertook a study to exam the practices boards should be adopting in providing effective oversight of the risk management process to support delivery of the strategy of the organisation. This report follows on from this initial study, and takes a closer look at how in practice businesses can truly embed risk management practices right across the organisation.

Embedding risk practices successfully can be challenging. A key issue is how we translate the management of risk from a theoretical exercise to an activity that has resonance and meaningfulness right across the organisation, at all levels. For risk management to be truly effective, it must be managed as an inherent part of delivering day to day business activities, which is why the application of risk management processes must occur at all levels of the organisation. This requires significant communication, collaboration and coordination across the business. However, no two organisations are the same, and the ways in which sound risk management practices can be established varies from business to business, taking into account a wide range of situational and cultural aspects.

We hope this report provides sensible reflections for organisation leaders at all levels to reflect on their own current practices in embedding risk management across their organisations. These considerations, as the report demonstrates, can apply both formally and informally, and it is essential that organisations consider their own unique circumstances, challenges and opportunities in applying these effectively.

Contents

Executive summary

Organisations in every sector, whether large or small, simple or complex, invest time and resources in managing risk. Effective risk management is an essential element in the success or failure of these organisations, but there remains much to learn about what actually constitutes effectiveness.

ACCA's 2018 report on board-level risk management practices, *Risk and the strategic role of leadership*, highlighted the significance of risk in the boardroom and how boards organise their risk management activities to inform strategy and governance (Ashby et al. 2018). This report investigates how board-level risk taking and control objectives translate into the risk management activities performed within organisations. The aim is to understand how these risk management activities are embedded to ensure that staff across the organisation collaborate and co-operate to manage risk in a manner that is consistent with the board's risk taking and control objectives.

Effective risk management within organisations can only be achieved when staff are willing to engage in risk management activities to achieve the board's risk taking and control objectives. In short, risk management cannot be effective if it is not embedded.

The project is based on:

- four in-depth case studies, which included documentation reviews, site visits and 34 interviews across a range of business functions
- two focus groups, consisting of a number of risk management professionals, and
- input from the ACCA's Global Forums, with particular thanks to the Global Forum on Governance, Risk and Performance.

The research shows that although the case study organisations had similar risk management objectives, the paths they took to embedding risk management varied according to the external environment in which they operated and a range of internal factors, such as leadership tone and the success or failure of past risk management initiatives. Organisational paths varied in the risk management mechanisms used and, in particular, the formality or informality of these mechanisms.

Communication is vital. This includes communication between business units and functions, as well as communication to/from the risk management function and internal audit function.

Key findings include the following.

- Effective risk management requires the use of complementary formal and informal mechanisms. Formal mechanisms include risk registers, control assessments, internal audits and risk reports. Informal mechanisms include social networking and sales/influencing techniques.
- Communication is vital. This includes communication between business units and functions, as well as communication to/from the risk management function and internal audit function.
- The risk management function has a pivotal role in communication and building risk management relationships. The function operates as a nexus for risk management communication, facilitating such communication between business units and functions and to/from the internal audit function and board/senior management. A risk management function that cannot build effective relationships across an organisation will not be able to embed effective risk management practices.
- The risk management function does not only design and implement risk identification, assessment and reporting tools; it must also work hard to explain and even sell the benefits of risk management to the wider organisation.
- Every case study organisation struggled with the requirements of a pure 'three lines of defence' model for risk governance. The authors propose reformulating the three lines model to create a less segregated, 'modes of accountability' approach.

Towards the end of the report the findings are consolidated into a conceptual model for embedding risk management in organisations. This 'risk gearbox' shows how formal and informal risk management mechanisms combine to create 'strategic thrust' to support the board decisions on strategic risk taking and control. There are also a number of recommendations for organisations looking to improve the effectiveness of their risk management arrangements.

Author biographies

DR SIMON ASHBY

While conducting the research, Dr Simon Ashby was Associate Professor of Financial Services at the Plymouth Business School. Previously he worked as a financial regulator for the UK Financial Services Authority (writing policy on risk management) and a senior risk manager in several UK financial institutions (covering both credit and operational risk).

Simon has a PhD in corporate risk management and has published many academic papers and industry reports in the discipline. His current research interests include board-level risk management and risk governance; cyber-risk management; risk culture; and the reputational effects of operational risk events.

Simon is a Fellow and former chair of the Institute of Operational Risk and a non-executive director and audit and risk committee chair of Plymouth Community Homes.

Simon is now a Professor of Financial Services at Vlerick Business School in Belgium, which provides high quality postgraduate education around the world (www.vlerick.com/en).

DR CORMAC BRYCE

Dr Cormac Bryce is a senior lecturer in Insurance and Risk at Cass Business School, City, University of London, and is a member of the Faculty of Actuarial Science and Insurance. His multi-method research spans areas from human behaviour in financial organisations to the effect of regulation on organisational behaviour within the aviation industry.

Cormac's recent research focus has been grounded in areas of the error-reporting climate, and the effects of risk events on the market sentiment of financial services organisations.

DR PATRICK RING

Dr Patrick Ring is currently a reader in financial services in the Glasgow School for Business and Society at Glasgow Caledonian University. He is a qualified solicitor who, before entering academia, worked in the corporate area of private practice, and later as a lawyer with a large life assurer.

Patrick's teaching and research interests include financial regulation and compliance; operational risk management and culture in financial services; trust in financial services; pension policy and reform; and the retail financial advice sector.

1. Introduction

The management of risk is essential for every organisation. In a complex world, full of political uncertainty, changing technology, long supply chains, just-in-time operations, the vagaries of social media and an assortment of other factors, risk matters. Success or failure depends on an organisation's ability to take, mitigate and avoid risk or to exploit, recover and learn from unexpected events when they occur.

ACCA's 2018 report on board-level risk management practices, *Risk and the strategic role of leadership*, highlighted the significance of risk in the boardroom and how boards organise their risk management activities to inform strategy and governance (Ashby et al. 2018). This follow-on report moves on to investigate how board-level risk-taking and control objectives translate into the risk management activities performed within organisations.

Most organisations with more than a handful of staff will have someone who has responsibility for identifying, assessing, controlling and reporting on risk. As organisations grow this individual may become a full-time risk manager and additional staff may be recruited to form a risk management function. In larger organisations, hundreds of staff may have full or part-time risk management roles covering different risk types or business areas.

Risk management is, however, about much more than the risk manager or risk management function. Risk is present in every organisational process, activity or decision. This means that all staff will have some responsibility for taking and controlling risk, the management of which is an integral part of the organisation's success or failure.

No matter how good a board's strategy and risk focus, or how deep its concern for stakeholder value and good governance, an organisation may fail to achieve its risk management objectives if staff are not engaged in these objectives or their risk-taking and control decisions are uncoordinated. It is here that embedding risk management is essential. 'Embedding' is about organising risk management activities to engage staff in the management of risk, and coordinating their risk taking and control decisions.

This report investigates how four case study organisations organise their risk management activities to achieve their objectives. Organisation is about more than formal structures, policies or procedures. Organisation is both formal and informal and both are necessary to ensure stable and effective results. For example, a risk-assessment and reporting tool, such as a risk register, provides a common formal mechanism for organising risk management, but the register may produce inaccurate or incomplete information if staff do not understand how to use it or perceive it as bureaucratic. It is here that the informal organisation, such as social networks and trust, comes into play.

The aim of the report is to identify the challenges that the case study firms have encountered when organising their risk management activities, and to share good practice. Each firm started from a similar position (limited organised risk management activity) and all are working to increase the organisation of their risk management activities to achieve goals such as organisational efficiency, stakeholder welfare, compliance, and reputation protection. Nonetheless, the paths that they have taken vary and reflect differences in their economic contexts and their organisational and risk cultures. This provides a wealth of practice that other organisations can use to improve their organised risk management activities.

Organisations make decisions about risk taking and control before they know what the outcomes will be. This means that all decisions on matters of risk require a leap of faith.

Case studies provide a deeper insight into the formal and informal aspects of organised risk management activity. A questionnaire survey or a broad-based semi-structured interview approach, as in the first report (Ashby et al. 2018), may not have shown the complex interplay that can exist between the formal and informal organisation. While the present report draws upon four cases, including 34 interviews, the findings are applicable to a wide range of organisations. This is not least because, despite considerable differences in their sectors, size and culture, they each faced very similar challenges, even though the solutions they have chosen vary. As with the previous report, it is for the reader to decide how to apply the findings to their own organisational context.

1.1 THE RISK MANAGEMENT CONUNDRUM

> *'I've worked in first line, second line and third line, and there is always, clearly, a healthy tension. But, from a first-line perspective, the guys just want to get on and run the business and this type of [risk management] activity can just be seen as an administrative frustration, an overhead that doesn't actually add any value'.*
> Business Manager

Organised activity of any form requires time and effort. Forms must be completed, reports produced, meetings attended and social relations developed, trust built and the benefits of various tools and processes must be 'sold'. Organised risk management activity is no different, but here two additional problems occur: the benefits of successful decisions about risk taking and control may not be realised for a long period of time and may be intangible.

Organisations make decisions about risk taking and control before they know what the outcomes will be. This means that all decisions on matters of risk require a leap of faith. Even the most obvious decisions may have unexpected outcomes. A new product may seem destined to succeed, but something may turn consumers against it. Equally, apparent improvements to health and safety may have unintended consequences. To make matters worse, the outcomes of a decision may be intangible, especially when they relate to a reduction in downside loss events.

The benefits of a decision on a specific risk are often apparent over time. An organisation can usually tell if a new product or efficiency improvement is successful or if a merger or acquisition is profitable. Such decisions will affect revenues or expenditures in a tangible way. But what about the implementation of enhanced risk reporting arrangements, a more complex risk register or the completion of internal audit actions – how are they connected to the achievement of organisational objectives? Especially, how do they affect the one thing that often matters the most – improving the bottom line?

Well-designed and appropriate risk management activities should, in theory, add value to any organisation. Every risk or accountancy professional should know that. The conundrum is that, in practice, this value may take time to materialise, if it becomes visible at all. As a result, asking busy staff members to invest tangible and immediate time and effort in organised risk management can be very difficult. Why should they invest this time and effort on activities that they perceive to be bureaucratic and distracting when they could spend these resources on apparently more interesting activities that provide more immediate and tangible benefits?

Most risk management professionals have encountered resistance to organised risk management activity, and witnessed this conundrum first hand. The risk management professionals we interviewed for this report were aware of the conundrum, and took steps to address it. Embedding is a key strategy. The task is to support staff at all levels below the board to appreciate the benefits of organised risk management activity and understand that these benefits will not only help the wider organisation, but also facilitate all staff in their roles.

We would also encourage those with deep-seated views to reconsider these in the light of the real-world experiences of organisations. There is no single best way to embed risk management in organisations.

An organisation with fully embedded risk management will accept organised risk management activity, even though the benefits may not have been realised or will remain intangible. This, of course, represents a holy grail and few if any organisations will achieve this ideal. Nonetheless, it is possible to move towards this goal. Each of the case study firms was on an 'embeddedness journey', albeit that they were all at different stages.

1.2 WHAT WE ALREADY KNOW ABOUT EMBEDDING RISK MANAGEMENT

Research into embedding risk management activity is not new. This report builds on and extends this literature. From the existing literature, we know that risk management activity requires a blend of formal and informal organisation. What is not yet understood is how this blend can vary across organisations or the factors that may influence this blend. In addition, understanding of concepts such as risk appetite and risk culture is at a very early stage and much of the existing literature does not examine how activities that focus on risk appetite or risk culture may influence the broader mix of organised risk management. For the interested, we provide a brief review of the academic literature on these issues in Appendix B.

From a practitioner perspective, we appreciate that there is an even bigger literature on the subject of embedding risk management, including an array of maturity frameworks, regulations, codes and standards. We are also aware of some strong views among researchers on topics such as risk governance and tools such as the 'three lines of defence' approach. While mindful of this literature, we argue that the best way to understand good practice is via direct observations conducted in a thorough and neutral way. Hence, the resulting suggestions for practice (Section 4) are based upon what the case study interviewees and focus group participants said about things that they have done that have worked or not worked. It is for the readers of this report to select the practices that may work for them or their organisation. We would also encourage those with deep-seated views to reconsider these in the light of the real-world experiences of organisations. There is no single best way to embed risk management in organisations.

1.3 RESEARCH AIMS, OBJECTIVES AND APPROACH

The aim of the project was to build on the ACCA's first *Risk and the strategic role of leadership* report (Ashby et al. 2018) on board-level risk management activities, to investigate the risk management activities that take place below the level of the board and to share good practice. These activities encompass the formal and informal aspects of managing risk and include risk policies and governance arrangements; risk appetite statements; risk management processes, procedures and tools; communication flows; committees; and work on managing risk culture.

The specific objectives were as follows.

1. To identify the risk taking and control objectives set by the board and senior management.
2. To analyse how risk-taking and control objectives are communicated and understood across the organisation.
3. To identify and assess the processes, tools and other structures that are used to identify, assess, control and report on risk taking and control across the organisation.
4. To investigate the nature and efficacy of any management sub-systems for risk appetite, risk culture and the exploitation of opportunities, including roles and responsibilities for these systems.
5. To understand how staff across different functions coordinate and collaborate to support the organisation's approaches to risk taking and its control objectives.

2. Project methodology

The findings from this report come from four in-depth case studies. These case studies cover different industry sectors and differ in size and complexity.

Two had relatively established risk management activities and two were in the process of implementing new activities, including risk appetite frameworks, risk-assessment tools, risk reports and IT systems for collecting, storing and analysing risk management information. Each case study included interviews with people from the risk management function, a senior manager or executive with responsibility for risk management, and representatives from front-line business functions and internal audit.

The interviews took place on-site and in person, with only a few exceptions where a phone call was necessary owing to the unavailability of staff during the site visit. Interviews were semi-structured (using open questioning to allow the interviewees to focus on the themes important to them) and followed an agenda appropriate for the role of each individual (director, first-line business management, second-line risk management or third-line audit). To facilitate analysis, interviews were recorded and transcribed. Two, and occasionally all three, of the researchers were present at each interview to control for interviewer bias and to ensure that each interview was as complete as possible.

To improve research rigour further, two focus groups commented on the draft findings in February 2019. These focus groups consisted of risk management experts and industry association representatives.

Appendix A provides a summary of each case and a list of the interviewees and their roles.

Budget limitations meant that the research focused on UK-based organisations. The researchers would encourage researchers in other countries to build on the findings and explore whether they remain valid in other cultures.

3. Findings

While completing the case studies and searching for recommendations for good practice, it became clear that there is no single approach to embedding risk management. Success depends on how well the formal and informal risk management arrangements of the organisation align with its culture and strategic objectives.

That said, we did observe a range of good practices, particularly in relation to how the risk management function works with other business areas and how the board and senior management communicate with and receive information from the business functions, including risk management and audit.

3.1 BALANCING FORMAL AND INFORMAL RISK MANAGEMENT TO ACHIEVE STRATEGIC OBJECTIVES

'All of the thinking and the conversations around that, you need that framework there to be able to do it. But the important stuff is not the bit of paper with all the output on, it's the conversations you have to fill that bit of paper in, if that makes sense?' (Risk Manager)

3.1.1 Combining strategy and risk

In *Risk and the strategic role of leadership*, we found that that boards adopted more or less formal approaches to assessing the risks associated with choosing or not choosing specific strategic options, and that such discussions were not necessarily structured in a formal way (Ashby et al. 2018).

Our findings in the present study confirmed this position, representative of the 'principled–prescriptive' spectrum outlined in that earlier report:

> *'I think we get challenged on it... every now and again. Okay, you guys have got this great strategy, but how have you assessed for risk?...we probably do it quite implicitly, but we're not good at doing that explicitly'.*
> Risk Manager

In the previous report, we also found that employing the notion of 'risk appetite' can help organisations improve strategic decision-making. In the case studies, risk appetite featured in discussions and in some organisations there was a focus on risk appetite as a means of supporting the development and embedding of risk management in the business.

In one of the cases, work had been done both to articulate risk appetite across the business and to put quantitative measures in place to assess that risk appetite; and in another case, the firm had based a new risk management framework on a series of risk appetite statements. There was evidence that risk appetite statements were being used to 'filter' risk registers containing an apparently high number of risks, helping the business to identify and focus upon the most important risk issues affecting its strategy. As risks are reported within the business, this helps focus attention and ensure that the key issues are easily identifiable to senior management and the board, especially where risk is only one item on a full board agenda.

Nonetheless, driving this risk appetite down to business level was still in its early stages for some of these organisations, and so it was clear that more work would be required to employ the concept of risk appetite effectively as a means of embedding risk management within the business.

3.1.2 Formal and informal organisation

Organisations have to coordinate the activities of various departments, functions and individuals. Effective coordination is essential for success and the creation of value, via the achievement of organisational objectives.

Activities are coordinated via formal and informal mechanisms, which reinforce

> Formal mechanisms provide a tangible management structure, while informal mechanisms help people to accept, understand and operate, and refine the tangible management structure.

each other to create efficient and reliable processes for the production and delivery of products and services.

Formal mechanisms provide a tangible management structure, while informal mechanisms help people to accept, understand and operate, and refine the tangible management structure.

In each of the case studies, we identified a range of formal and informal mechanisms for organising risk management activities. Table 3.1 provides a list of the main mechanisms discovered. (Note: this is not an exhaustive list.)

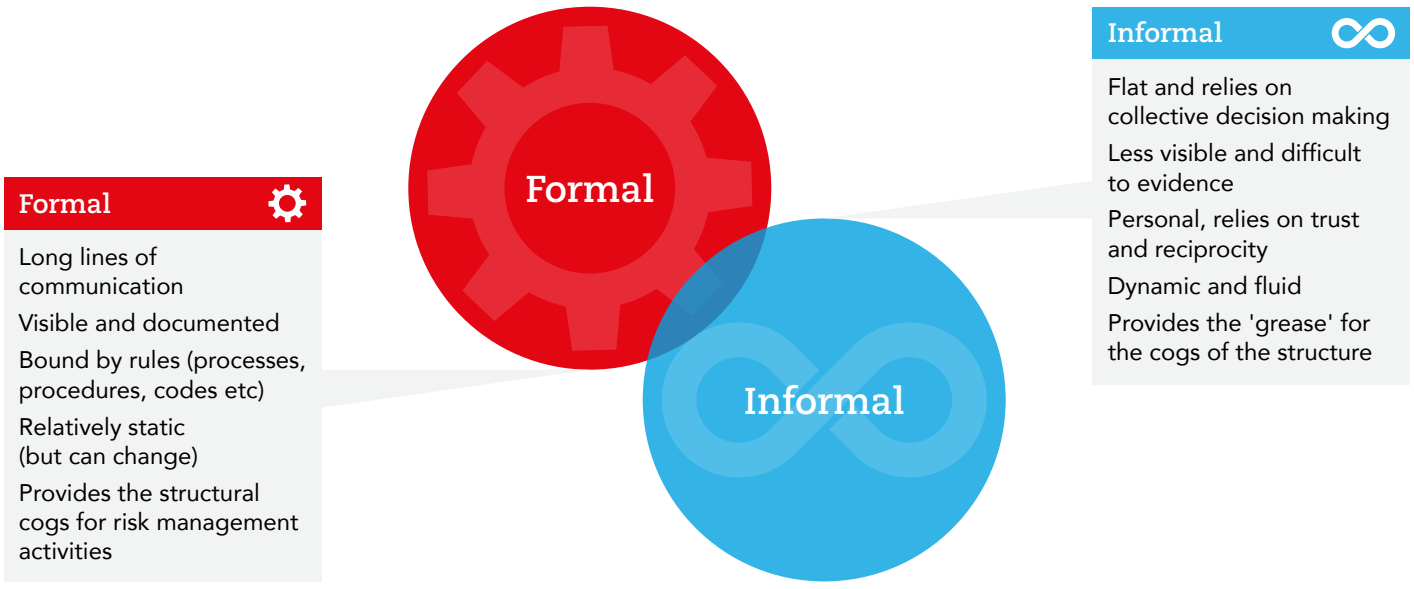
In each of the case studies, the formal and informal mechanisms were complementary and overlapped to a degree, as illustrated in Figure 3.1.

From a risk management perspective, the formal mechanisms used by organisations provide a visible and stable structure. The informal mechanisms support the execution of these formal mechanisms and help to fill in any gaps. Both are essential and used in tandem by each of the case studies, though we observed differences in the balance of formal and informal mechanisms. This is explored further in section 3.1.3.

TABLE 3.1: Common formal and informal mechanisms for organising risk management

FORMAL MECHANISMS	INFORMAL MECHANISMS
Risk management policy	'Tone from the top' and the actions of executives and senior management
Risk appetite statement and exposure limits	Risk facilitation by first- and second-line risk specialists
Management committees (risk specific and general)	Phone calls and face-to-face conversations that cut across hierarchical layers
Ownership and accountability, for example, risk and control owners	Risk forums and small group huddles
Risk specialists (1st and 2nd Line)	Walking the floor
Process mapping and failure point analysis	Idea sharing (to identify common concerns and good practice)
Risk registers	Weekly horizon scanning updates
Control effectiveness testing	Mentoring, especially second-line risk function mentoring first-line risk specialists
Loss and near miss data collection	Explaining and selling the benefits of formal mechanisms like risk registers
Risk reports (risk matrices and risk and control indicator reports)	Other activities to influence attitudes, perceptions and behaviours
IT systems for collecting, analysing and reporting risk information	
Internal audit reports and action plans	

FIGURE 3.1: Formal and informal organisation



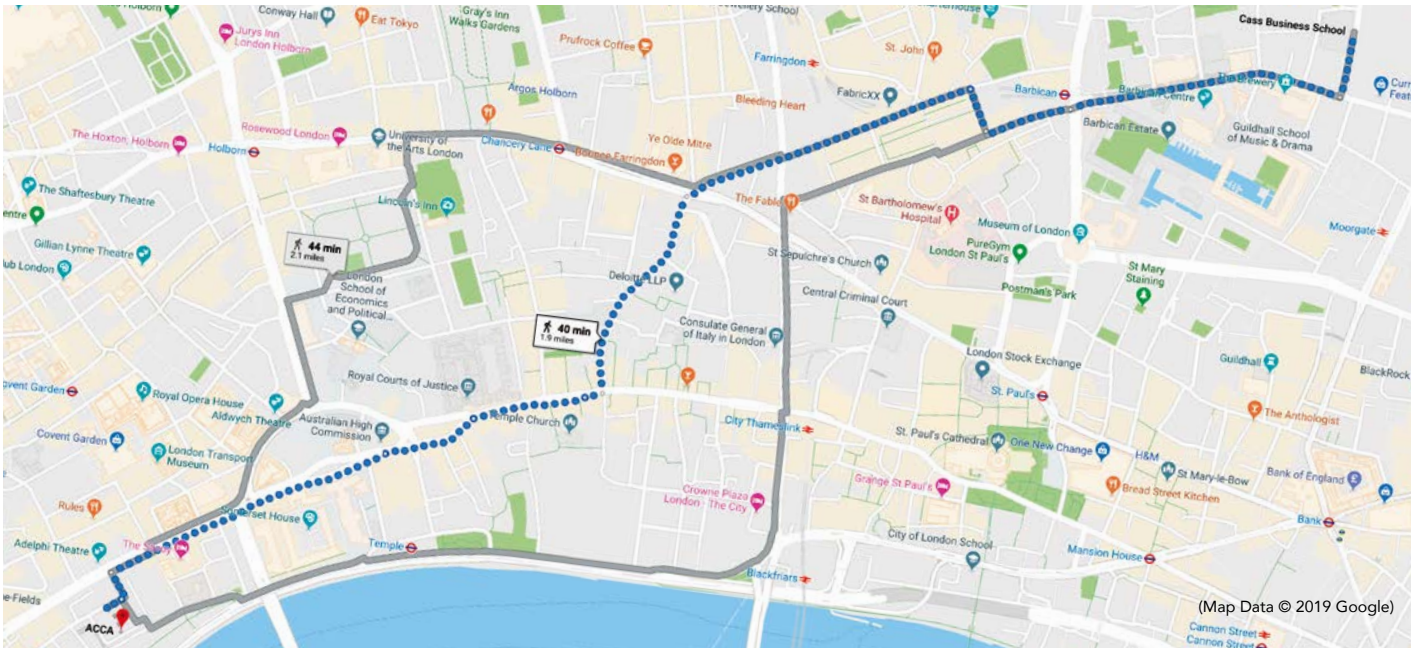
Common risk management objectives included: encouraging greater first-line ownership of risk; more proactive and less reactive risk management activity; reduced administration time and bureaucracy; and driving culture change.

3.1.3 The risk management journey

Each case study organisation had risk management objectives that were linked to the organisation's strategic objectives. The risk management objectives were very similar across the cases. Common risk management objectives included: encouraging greater first-line ownership of risk; more proactive and less reactive risk management activity; reduced administration time and bureaucracy; and driving culture change.

Though the case study organisations had similar objectives and started from the position of little or no explicit risk management activity a few years ago, each took a different journey, using various combinations of formal and informal mechanisms. This is like taking a different route from a common starting point (Cass Business School) to the same destination (ACCA offices at the Adelphi) as seen in Figure 3.2.

FIGURE 3.2: Similar objectives, different paths



Case example: Expert facilitation to support risk reporting and decision-making

This case study firm implemented a corporate risk management approach two years ago and is continuing to improve the approach. It has a suite of division- and function-level strategic risk registers and action plans and a board-level enterprise-wide risk register and action plan.

Risk reports for the audit committee and senior management meetings at operating division and head office function levels are produced using the information contained on the registers/action plans. In addition, the organisation is implementing a risk appetite and risk-tolerance approach, which sets out target risk-exposure levels (risk appetite) and maximum tolerable levels of exposure. The organisation does not have a risk management IT system, but is considering the purchase of one.

The risk management function works as a business facilitator, a form of in-house risk consultancy. The team meet with first-line risk specialists and senior management across the organisation to help them identify, understand and control strategic-level risks. This consultation includes attendance at formal meetings and many informal conversations on the phone and face to face. Close contact with first-line risk specialists and senior management (the risk management team are able to talk to all levels of the hierarchy) has built high levels of mutual trust and respect. As a result, the risk management function has ensured engagement in the formal risk management approach despite significant levels of resource constraint across the organisation. Historically, formal risk management activity was viewed as *'administrative'* and *'bureaucratic'*, but the risk management function is using soft skills (facilitation, networking, relationship building and selling) to change this mindset: *'it's all about relationships'*. ■

We learned that changing the design and mix of formal and informal risk management mechanisms can, in itself, help to embed risk management in an organisation.

The factors that influenced the route taken by an organisation were external and internal. Table 3.2 summarises the factors that we observed.

These factors combine to create a unique history for an organisation, a history that includes learning from the successes or failures of earlier risk management activities. Such learning was a significant part of the internal factors. As factors change, especially when previous risk management activities are perceived as a success or failure, the journey continues. Interviewees from all the organisations talked about risk management as a journey. Risk management activities rarely stay the same for long. Organisations must refine these activities to adapt to changes in their external and internal environments and the effect that these changes may have on their risk exposures and strategic objectives.

We learned that changing the design and mix of formal and informal risk management mechanisms can, in itself, help to embed risk management in an organisation. Providing change in risk management mechanisms is not too frequent, which can cause change fatigue (something we observed in one of our cases), it can help to keep risk management fresh and provides an opportunity for the risk management function to promote risk management by generating interest in a new tool, report, process or governance structure.

'It's easier to sell something that's new than just trying to force the same old stuff down peoples' necks that they've maybe seen before and they haven't engaged with. So, by revising what we've done and branding it all as our new approach, I think people are keener to hear what we're doing. And we've tried to simplify it, we've tried to make it easier for people, which I think is helping as well'.
Risk Manager

TABLE 3.2: Factors influencing the risk management journeys of the case study organisations

EXTERNAL FACTORS	Regulation and supervision, which tend to encourage more formal risk management activities
	Events which affected the reputation of the organisation or its competitors
	Pressure from shareholders
	External audit recommendations
INTERNAL FACTORS	Appointment of a new audit or risk committee chair
	Appointment of a new chief risk officer (CRO) or equivalent
	Creation or expansion of a group risk function
	The skills and past experiences of the CRO or other senior risk managers
	The rapid growth of an organisation, including via merger or acquisition. Organisational processes, including risk management activities must keep up
	Resource constraints in the first or second lines
	Internal audit recommendations
	Disparate and uncoordinated risk management activities across the organisation
	Previous risk-assessment or reporting tools perceived as ineffective or bureaucratic
	Obsolete or unsupported IT systems for risk management

Case Example: Two organisations – different journeys

When we visited these two organisations, they were implementing new risk-assessment and risk appetite tools. Both organisations were resource constrained and hoped that the new tools would reduce bureaucracy and help management to focus on the most significant risks. These included risks that were significant at the enterprise-wide and business unit/function level.

A further shared risk management objective was to enhance the control of risk by first-line management. In each case the pressures of the 'day-job' were a problem. In the first case study this manifested as a 'non-accountability culture' where managers were reluctant to take responsibility for certain risks or controls because of resource pressures that might mean that taking such responsibilities would entail more work.

'I have seen the behaviours in the first line that people don't like to be open when things aren't working well. People don't like the colour red, they don't like having events. And they don't like raising events because a), it acknowledges that something's gone wrong and b), it means they've got admin work to do. So there's a real culture of people trying to avoid managing risk or identifying risk' (Risk Manager).

In the second case study, first-line management were willing to take responsibility for managing risks, but did not always complete the actions required. Here the culture was described as 'can do' and 'just go and do it'. First-line managers were quick to accept potential risk or control problems, but this enthusiasm could soon wane, because of the complexity of a problem. Problems were not always addressed in a permanent manner:

'We do a lot of things in our organisation where, just go and do it and see if it works, and then we… say, "well, that was really, really good" but we don't really know it's really, really good because we didn't actually put the correct infrastructure before we actually try something out. So we get lots of good ideas and we're in a very dynamic environment so people say, "we've got a really good idea, we're going to go and tackle a problem here and then we're going to have really good outcomes from that", but they don't really think about what they wanted. They don't know how they're really going to measure and capture [the results] before they actually go out there and do it. So it's almost like we're on a bit of a back foot and we have to say, okay, before you go and try something new, you need to capture how you're going to do it, why you're doing it. What's the outcome from that? What will it affect?' (Risk Manager)

While the two organisations shared similar objectives, the external and internal factors that drove the changes to their risk management activities were different. The first was implementing a significantly more formal risk-assessment/risk appetite approach, with detailed process mapping, evidence-based control testing, risk appetite metrics and a new IT system. In contrast, the second was implementing a much less formal risk-register/risk appetite matrix approach that relied on management judgement and was recorded on spreadsheets.

Key internal factors that influenced the formal/informal mix in both cases were the personalities and past experiences of the senior risk management team. In the first case study, the new CRO had come from an organisation that worked within a heavily regulated jurisdiction where rigorous and formal control testing was perceived as important. The other members of the senior team also came from organisations that had emphasised formal risk management. In contrast, the senior risk management team in the second case study placed much more weight on informal mechanisms.

Both organisations were subject to significant external scrutiny. Nonetheless, only managers in the first case study talked about regulators driving a relatively formal risk management approach:

'…we're regulated and we have got to do things right. So you've got to have governance in place and it's got to be strict…'. (Risk Manager)

Both organisations used a range of informal mechanisms to help reinforce the risk assessment and appetite approaches that they had designed. The second case study, however, gave much more emphasis to these mechanisms and was more involved in the work of its first-line staff. Its risk management function acted as a risk management facilitator and helped the first line to identify, assess and control significant risks. This included help implementing action plans and acting as a 'critical friend' where necessary. It also required a lot of 'hand holding'. In contrast, in the first case study, the senior management was not as close to those in the first-line and gave more emphasis to a formal second-line risk-oversight role. Though it did not apply a strict 'three lines of defence' approach, risk management function staff admitted that they were acting in a business partner capacity during the implementation phase of the new risk management mechanisms. This was to provide training and support for first-line staff, who were unfamiliar with the new mechanisms. ■

Effective risk communication requires a blend of both the formal and informal – each of which complements and supports the other to enable effective risk management across the organisation.

3.2 COMMUNICATING FOR EFFECTIVE RISK MANAGEMENT

3.2.1 The fundamentals of effective risk communication

There were clear formal structures of communication up and down the organisations in all our case studies. Their specific nature depended upon the size of the organisation and the nature of its activities but, in all cases, they were important for disseminating 'tone from the top' and escalating key risk issues up the organisation. We were told that complex committee structures could slow down communication, affecting the agility of the organisation in dealing with risk issues.

We also found that more informal lines of communication, including the 'dotted lines' between the risk function and senior executives and board members, are also essential for successful risk management. Effective risk communication requires a blend of both the formal and informal – each of which complements and supports the other to enable effective risk management across the organisation. But the important point is that the self-reinforcing combination of the formal and informal lines of communication is needed for risk management to be effective.

Our research uncovered three significant requirements for effective risk communication. Firstly, it is important to ensure that formal committees and reporting structures work as intended for transmitting, and allowing staff to act upon, appropriate risk information. Secondly, the integral nature of 'informal' communication to successful risk management means that 'informal' should not be seen as a matter of 'happenstance', and the relationship-building skills of the risk management function are important here. Thirdly, when working with the business units, the risk managers have to think carefully about how they talk about risk.

3.2.2 Effective structures of communication

Committees need to receive the right information at the right time, as well as having the right conversations in relation to that information, if they are to work effectively to support the strategic objectives of the organisation. We heard of an audit committee where the dynamics of setting the agenda meant that the challenge at that meeting was not as effective as it could be. By contrast, in another case study, the organisation's 'conversation culture', although generating a close relationship between the risk management function and executives, sometimes meant that the former did not feel as informed about the strategy of the organisation as it might have through more formal discussions. This reflects our previous ACCA research (Ashby et al. 2018), suggesting that informal communication lines may sometimes benefit from more structured 'anchor points', providing a level of formality sufficient to ensure that key messages or pieces of information are transmitted and received.

Case example: Ensuring that committees communicate effectively

In one of our case studies, we found that in the past there had been some concern that the audit committee had suffered from an overload of information reporting into the committee, and that this might hamper in-depth scrutiny by the committee.

Nonetheless, the appointment of a new member of the board with an interest in risk management and a new chair of the audit committee brought significant change in how risk management objectives were being communicated and understood.

'So in the very early days of...our audit and risk committee, there wasn't a lot of debate about risks or audit activity. It was like, "thank you very much for bringing that to my attention", rather than having an active discussion about it. So that has completely changed. There's a lot more discussion. There's a lot more awareness about it now. People are taking about it. People proactively approach you for help and assistance…

'More importantly, when they took over as C-suite Manager they immediately put in place a structure…that made quite a big difference, because we then had visibility at senior leadership meetings, and because we have that one individual who wasn't conflicted with having any other responsibilities – and, you know, that's their core, and they're able to take the issues that we experienced and air them at [board meetings]. So there's a lot more visibility of problems, and there's a lot better consideration of it, too'. (Risk Manager) ■

The risk management champion can effectively disseminate 'tone from the top' to the front line of the business. In one case this led to the development of an effective information cascade through 'dedicated individuals' in each team.

Individual personalities can also influence the formal communication process. In one case, the chief risk officer regularly holds 'challenge' sessions with business managers where their risk-assessment and control-testing activities are discussed. This has had the effect of making clear to the whole business the importance of these activities and the output expected.

At the same time, for the right conversations to take place, the right people must be at the right meetings. In one of our cases, 'execution groups' had been formed to discuss risk assurance across specific functions of the business. Initially, the risk and compliance execution group had included representatives of ExCo, the risk management and compliance functions and business units. A decision was made to change the composition, so that the group consisted only of the risk management and compliance functions.

> *'Now, you lose something. You lose quite a lot if it's just a second-line forum. Second line can have a conversation themselves, but if that's a challenge forum in your business, if you're not speaking with the ExCo, if you're not speaking with your business, then you can't evidence [that] you're doing sufficient challenge'.*
> Risk Manager

Because the committee was not having the 'challenge' discussions it needed to have, it reverted back to its initial composition.

Enhancing the structure – the importance of risk champions/hubs

One means of extending the communicative power of the risk function was by adapting the structure of risk management and communication through the use of risk management champions or hubs (the latter being a risk management function group, rather than a designated individual, within the business unit). Situated in the business unit, these champions/hubs bring an understanding of how best to embed risk management in the business unit and, importantly, use their personal relationships with other front-line staff to achieve this. The risk management champion can effectively disseminate 'tone from the top' to the front line of the business. In one case this led to the development of an effective information cascade through 'dedicated individuals' in each team. It was also noted, however, that practice could differ between business units, resulting in variations in the effectiveness of risk communication.

Individuals acting as champions, or as part of a risk management hub, often had a number of other roles in the business unit, so their capacity for undertaking their risk role effectively could be limited, and we found examples where there was variability in their effectiveness within organisations. It is therefore important that if the risk management function is extended using risk champions/hubs, they are adequately supported and resourced to carry out this role.

Case example: Using risk champions to embed consistent practice

One of our case study organisations has a network of first-line risk specialists. Each operational division and head office function has a team of one or more risk specialists. These specialists support the completion of risk assessments and control effectiveness testing.

They also provide subject matter expertise in areas including human resources (HR) risk management, cyber risk, data protection and finance. Having first- and second-line risk specialists creates synergies, the second line bringing conceptual risk management expertise to complement the first line's local knowledge:

'I think sometimes, it's a genuine discovery on both sides, so the risk team don't necessarily know what they're trying to ask, but we'll apply our expertise and come up with what we think the right answer is'. (Risk Champion)

The front-line risk specialists were instrumental to implementing a new process-based approach to risk assessment and controls testing, as well as a complementary IT data management and reporting system. The first-line risk specialists did this through informal channels working on a one-to-one basis with local risk and control owners to help them complete the new assessments and populate the system. In turn, the first-line risk specialists had regular one-to-one contact with the second-line risk management function, which had designed the new risk-assessment approach and system.

During the design phase the first-line specialists and risk and control owners were consulted on the new approach, system and related documentation. In addition, the first-line specialists and owners provided feedback during the initial implementation phase. This helped to refine the approach and reduce the time required to complete the new assessments. It also helped to improve the accuracy of the assessments and embed the new approach across the organisation.

'So, that's meant that because we've all had to work together to build those documents out, we all understand much better what we're meant to be doing. And risk management becomes part of how you do your job, rather than it being something that the risk team do or something that somebody else worries about. It's absolutely intrinsic to what we're doing, which is exactly the outcome I think everybody strives for'. (Risk Champion)

This organisation encountered some problems with the use of first-line risk specialists. Because of the informal nature of relations between the second-line risk function, first-line specialists and risk and control owners, different divisions and head office functions varied in how they implemented the new risk assessment approach. This led to some inconsistencies and inaccuracies, reducing the effectiveness of the approach. Historical differences had also emerged in relation to the design of risk reports and the effectiveness of local control environments. To help combat these inconsistencies a change was made to the formal reporting line of first-line risk specialists: they now all report into a single senior manager at group level. In addition, the organisation was considering implementing a monthly risk forum for first-line risk specialists. A forum would save the second-line from having to organise large numbers of one-to-one meetings to repeat information to different first-line risk specialists. It was also hoped that a forum could be used to share learning and good practice across the first-line risk specialists and address the inconsistent practices observed in some areas. ■

Across all our case studies, informal lines of communication were vital in underpinning the more formal organisational structures that supported risk management.

3.2.3 The importance of the informal: building relationships

'I think if it was just the formal, it wouldn't be as embedded in the business. I think because there is that informal ability to pick the phone up to somebody who might help you chew a problem over, it just works'.
Board Member

Across all our case studies, informal lines of communication were vital in underpinning the more formal organisational structures that supported risk management. The role of the risk management function is key in developing informal lines of communication through its capacity for building relationships across an organisation. The outcome is an increased awareness of the role of risk management; and it means that colleagues across the organisation, in carrying out their roles, are more likely to pick up the phone, walk across the room, or drop an e-mail about specific issues or concerns they may have. In our research, risk managers made time to develop effective working relationships across the business: *'I have yet to meet a successful risk person who can't make good, strong business relationships'.* (Board Member)

We found relationship building to be key for effective communication between the risk function and board members. In one of four case studies, the risk managers had been able to take advantage of a change of personnel at board level which had brought in individuals more attuned to the importance of the risk management function. The development of this relationship resulted in an expansion of the risk management team and much greater visibility of the risk management function. One immediate effect was in top-level board and committee meetings, where risk became the first item on the agenda, ensuring that it also influenced subsequent discussions.

Likewise, in another case study, a risk manager highlighted the importance of having a supportive relationship with the chair of the risk and audit committees, which facilitated communication both up and down the organisation:

'[We] will have a very free and open conversation about what they want to see, how can we better improve the articulation of what we're doing. [They] very much see my role as eyes and ears in the business, that's their term. And I would say that's a double-edged sword. What I do feel [is that] I have is the confidence of the board through [named person] and through the others as well, who I have known for a long time. And I also know and have proven it, that if there's something that I'm concerned about, I can take it [to them]'.
Risk Manager

Case example: Importance of relationships for communication with the board

This case study illustrated that for the risk management function to be confident about how it is both feeding into, and being supported in communicating and implementing, the risk strategy of the board, the relationship between one particular board member and the risk manager was key.

This was a relationship that had developed over a number of years and on the basis of sometimes challenging conversations. Both recognised that their informal meetings enhanced how they fulfilled their roles in the risk management of the organisation.

'My [board member] is super engaged…it's really quite satisfying as a relationship. They will challenge points they know I wouldn't have thought of. And I'll come with challenge points to them that I know they wouldn't have thought of. And actually, what you get is a really clear ExCo view into what needs to be done, which is really helpful...So, you know, we can generate what we like, but then I've got a really strong one-to-one with the [board member], and if I can get it through them, the chances are I'll get it through ExCo' [Risk Manager]

'So primarily I see my role as being things like supporting the [risk manager], empowering them, acting as point of escalation, and providing a bit of marketing. In other words, fighting their battles, making sure they get the exposure they need, making sure they get the recognition they need, and that risk is taken seriously at an executive and a board level'.

'[It's also]…marketing to the executive committee and making sure that they understand and embrace risk management so that they will take it to their teams and then they do that through making sure people update their risk matrices or respond, raise and respond to risk events or build risk into project concept documents or key projects that the business is running…' [Board Member] ■

What was recognised in all the case studies was the importance of getting away from 'technical' risk language when dealing with the front-line business.

In communicating and developing relationships with front-line staff, it is important for the risk management function to relate the benefits of risk management to the objectives and targets of those staff. Such benefits can be improved outcomes in day-to-day business activity, as well as meeting broader business-level strategic objectives or helping to secure resources to improve efficiency in a business area (particularly important where there is no apparent immediate benefit to the business area, as otherwise frustration and lack of engagement may set in). Where positive outcomes are achieved in one area, this can ultimately 'spread the word' about the importance of good risk management: *'we have managed to somehow prove that actually we are worth their time, and we can do things for them and help them manage their business better, and they're now one of our best advocates'* (Risk Manager)

Role of trust

Relationship building is key to the development of trust, which in turn was found to be important for effective risk communication:

> *'Most people in the business, if they've got something they're not comfortable with, will come and speak to [a member of the audit and risk management] team because they know we're there to support them'.*
> Risk Manager

Trust is needed if staff are to feel able to approach the risk management function to discuss potential problems and issues that might draw attention to their risk management practice. It is equally important in reducing the likelihood that criticism will be taken personally when a business function is challenged about the effectiveness of its management of risk. In one organisation, the introduction of a new assessment tool for process risk meant that business units were having their existing practice questioned in depth, and this created challenges for those in both the business units and the risk management function.

> *'You need colleagues who are comfortable and prepared to talk about… what they do, what could go wrong. Even getting someone to…acknowledge that sometimes things can fail in their process is like, ah! … "it's okay, it's okay, it's fine, it's okay". …And they take something away from that, and you'd hope that they learn, maybe that they're more positive about it, going forward, in their outlook, and the culture starts to change…the practice reinforces the values'.*
> Risk Manager

3.2.4 Conversations about risk: 'risk talk'

What was recognised in all the case studies was the importance of getting away from 'technical' risk language when dealing with the front-line business.

> *'I rarely use the word "risk"…And we just ask the question: tell me what can go wrong? Tell me what has gone wrong and tell me what could go wrong?'*
> Risk Manager

Each organisation had a range of risk management tools, procedures, mechanisms and software to enable staff to manage risks in their business functions, but the embedding of that activity was most effective when it was not 'badged' as 'risk management' – which staff would sometimes treat as a signal indicating that this was not their responsibility, but the responsibility of the risk manager, or the risk champion/hub in their own area. *'If I label it as risk, I will hit a wall and that wall is, "no, we do business"'.* (Risk Manager)

Instead of using risk terminology, or referring to a risk management framework, the risk managers often talked with the front-line staff about how to become more efficient, or customer-focused, or simply about the right behaviours and attitude:

> *'Client language and conduct language would be very strong. People wouldn't really use risk language, but some parts of the business are very, are actually very, very strong in that regard…In a sense, risk isn't part of the language as such. It's about these other things, about…what's important to the business that drives the right behaviours, the right culture'.*
> Board Member

Risk champions/ specialists in the business units were particularly aware of the importance of 'translating' risk language into language that resonated with front-line staff.

This approach was characterised by one interviewee as follows:

> *'Actually, it's a bit Machiavellian really, but it's my job to help them help themselves, and risk management is a management competency…I think we are a function of an environment where the fewer times we use [the word] "risk", the more doors open. …. If they don't even realise they're doing risk management, even better'.*
> Risk Manager

There are obvious links between this approach to managing risk and the development of the attitudes and behaviours that have been identified as essential for developing the appropriate risk culture in any organisation (IRM 2012). For example, one interviewee mentioned trying not to talk about the 'three lines of defence': *'I just want people to think we are not against each other, we're all in the same company'*. (Risk Manager)

Recognising the interplay between risk, compliance and internal audit in the risk framework, it is important that the 'non-risk' language and messages coming from all these functions is framed in a similar way to ensure consistency within the business. Risk champions/ specialists in the business units were particularly aware of the importance of 'translating' risk language into language that resonated with front-line staff:

> *'If you need to put a message out, if you put a message out…in the layman's terms [of not] talking about strategy and criteria, and risk appetite, I actually say… we would appreciate if you did A, B, and C. And that message is out there'.*
> Risk Champion

What seemed to be clear was that this approach, using 'risk talk' that avoids mentioning risk, is a means of generating greater business recognition of how managing risk underpins the efficiency of the organisation *'Are we seeing much better discussions? I would say, yes'*. (Risk Champion)

3.3 OVERCOMING IMPLEMENTATION CHALLENGES

3.3.1 Creating risk value: managing the cost–benefit equation

> *'I'd much rather help the business get things right than tell them they've got it wrong'*
> Risk Manager

Although the risk management function within each case study was well known and, for the most part, well received by the rest of the business, it could suffer from a dilemma in identity. As a function within an organisation that may not have direct revenue-generating capabilities, the difficulty lies in being able to evidence 'value added' to the business while ensuring that opportunities are maximised and threats minimised. In the process of trying to meet these sometimes-competing outcomes, the risk management function can be seen by the business as stifling innovation, slowing down product development, and increasing the administrative burden on the business. This was succinctly expressed, where it was noted that the risk management function had re-engineered its approach to be more business facing and thus avoided these perceptions. *'I think what has really helped, is that they [risk management function] take feedback from the business...So, the risk reviews now are so much tighter, shorter, more focused than they were five years ago'* (Risk Champion).

Nonetheless, perceptions of the risk management function as an administrative burden are only part of the story, and rather naïve. In focusing only on the processes and procedures for minimising threats, which are easy to evidence, the value the risk management function brings to the seizing and maximising of opportunities, which is difficult to evidence, is likely to be underplayed and devalued by the business.

In a number of the cases studied, it was clear that these perceptions make identification of 'value added' by the risk management function more difficult for the business to assess.

This identity dilemma is accentuated in those organisations that place an onus on the minimisation of threats at board level, are heavily regulated, or that have immature risk management functions. As a result, the risk management function becomes more concerned with administering risk strategy and less with actually managing risks so that the business can meet its strategic objectives. In a number of the cases studied, it was clear that these perceptions make identification of 'value added' by the risk management function more difficult for the business to assess. This was highlighted explicitly in some cases: *'we have some departments who struggle to see the value and it's sometimes a bit of a challenge'* (Risk Manager). This only serves to reinforce misperceptions about the risk management function, inhibiting its inclusion in discussions and the sharing of risk-related information between the first and second lines of defence.

In the 'asset protection' example (see box), it is clear that synergy between the risk management function and the rest of the business, allowed for risks to be addressed in a way that was tangible, effective and timely. Such synergies are developed over time, as the risk management function becomes more mature, improves its understanding of the explicit risks faced by the business, and develops a relationship with the business that allows it to move from business partner to facilitator. It is at this juncture that 'value added' becomes conspicuous to the business, a position that some of our interviewees said they were already close to achieving. This creates a 'risk collegiality' between the first and second line of defence, which becomes more embedded in the business when the risk management function begins to take into consideration not just what is right for risk management, but also what is effective and feasible for the business. This 'value reciprocity' will only be maximised when the risk management function stops 'shifting huge piles of data on and off Excel spreadsheets' and facilitates the ownership and accountability of risks within the business. In doing so, risk managers will be freed to spend more time with business contacts, facilitating the advancement of risk-related conversations, and concentrating on maximising business opportunities and minimising threats to business strategy.

Several of the case studies indicated that IT resources are being deployed in assisting the transfer of ownership and accountability back to the business, although it was acknowledged that the roll-out of risk software and IT systems was by no means a panacea. Further, their implementation has financial and non-financial start-up costs that must be incurred before they begin to facilitate the kind of risk ownership that enables the risk function to realise greater 'value reciprocity'. Nonetheless, the ability to have an accessible system in place that facilitates and encourages risk ownership, transparency, and accessibility across the front line of organisations can contribute to the embedding of risk management in the business and provide clear lines of accountability and audit trails.

Case example: Asset protection for risk management 'value added'

Few would argue that the greatest asset to a business is its employees, and with over 400 million customers per year, and a proportion of those being unwelcome on site, protecting those assets is no mean feat.

In the face of increased assaults on staff and the ever-present risk of terrorist attacks in crowded places, the risk management team in one case study firm, in collaboration with the staff themselves, came up with a technological solution that formed part of a larger initiative for protecting front-line staff.

Security staff on selected pilot sites were provided with body cameras that act not only as a deterrent to assaults, but also as detective control in the evidence-gathering process. The success of this pilot led to its roll out across all the organisation's sites, leading to a marked decline in incidents.

The entire roll-out was funded through insurance premiums savings resulting from reduced claims from incidents. While this may not have had a direct influence on revenue generation, the 'value added' of this risk management initiative was clear to the business. While providing a safe and secure environment, the initiative also improved customer experience and gave security staff the confidence to add value as they hosted customers. ■

The aim is to embed day-to-day (risk) management where it needs to be undertaken whilst liberating the risk management function from being information aggregators.

'So, if you can sit and say…"I can send you a spreadsheet or I can show you a fancy dashboard that you can dynamically click on different elements and it updates" they're going to be more engaged in that, we find, than they would be [in] a spreadsheet…I can see the updates coming in a lot quicker than I used to'.
Risk Manager

The ultimate outcome is not to pass an administrative burden back to the business, but to embed day-to-day (risk) management where it needs to be undertaken and at the same time liberate the risk management function from being information aggregators, enabling it to support the business better, and allowing for better-informed managerial decisions at every level of the organisation. Understanding how threats and opportunities co-exist across the business, and engaging better with the business to help it exploit the opportunities and manage the threats, are the foundation stones by which the risk management function supports the organisation.

3.3.2 Accountability

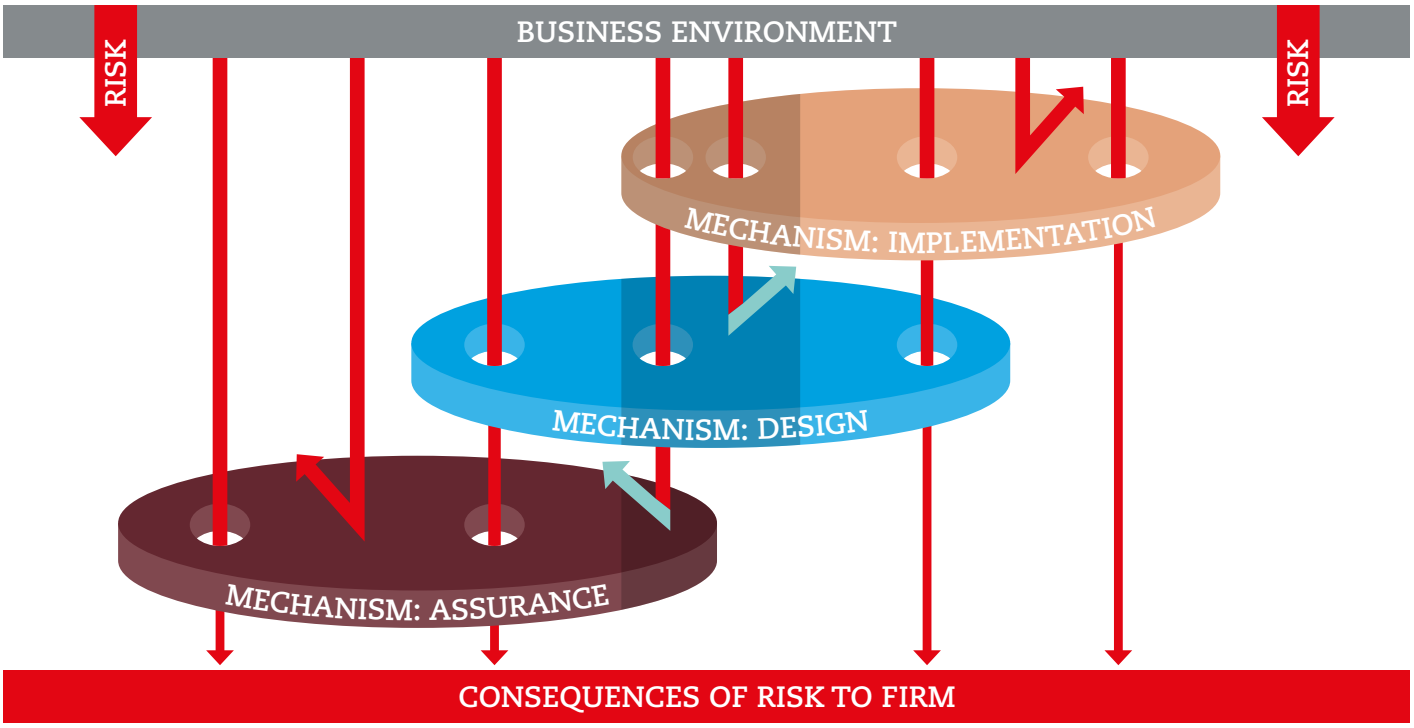
The 'three lines of defence' approach has become the dominant mode of risk governance in organisations. Regulators in sectors such as financial services are strong advocates and many risk management professionals also advocate this approach. In each case study firm, all the risk and audit function staff that we interviewed understood the approach, as did many of the first-line interviewees.

Though they understood the three-lines approach, however, none of the organisations had what could be described as a 'pure' three-lines approach. In addition, each one was aware of this fact and this divergence was a positive choice.

We understand that a three-lines approach can enhance risk governance, but what we observed in each organisation was a struggle to reconcile the theoretical ideal of a three-lines approach with the practical realities of implementing one. We have reformulated this model to consider modes of accountability, rather than lines of defence, which helps bring our observations across the four case studies into perspective. Figure 3.3 illustrates the three modes of accountability used by each of the organisations.

Within the three modes of accountability, the risk management function is accountable for designing the organisation's formal risk management

FIGURE 3.3: The three modes of accountability



Remaining approachable, to ensure that business managers came to the risk management function with problems or concerns at the earliest opportunity, was viewed as more important than a strict interpretation of the three-lines approach.

mechanisms (registers, risk matrices, etc.) and overseeing the risk-taking and control decisions that are made by other business units and functions. In turn, these business units and functions are accountable for using the mechanisms provided by the risk management function to help make risk-taking and control decisions that are consistent with the organisation's risk management and strategic objectives. The internal audit function is accountable for providing assurance that all risk-taking and control decisions and the risk management mechanisms used to support these decisions are appropriate.

An important difference between the three modes of accountability and the three lines of defence is that the former overlap in how accountability is distributed, though the degree of overlap can vary. This overlap is important, because it facilitates trust and cooperation across the three accountabilities. Trust and cooperation that can help to mitigate the adverse consequences of risks or exploit the opportunities that can come from risk exposures. The arrows which turn from red to blue in the shaded area where the three modes overlap illustrate potential threats which have been turned into opportunities.

We observed these variations within our case study sample. The use of business risk specialists/champions is one common reason for such overlap. These specialists/champions are outside the central risk management function but help to support its work. This can include by advising on the design of formal risk management mechanisms, and challenging the risk-taking and control decisions of other managers in their area. An additional source of overlap is the use of combined risk and audit functions, which we observed in two of our case studies. In terms of turning threats into opportunities we observed risk assessment and internal control tools being used to increase process efficiency or to speed up the development of regulatory compliant products/processes. We also saw risk and audit functions working with business function managers to help them make better (i.e. more profitable) business decisions.

Another strategy that can help embed effective cross working across the three modes of accountability is for the risk management function to create a collaborative, 'one team' approach. Despite one of our case studies being under regulatory pressure to implement a

Case example: The dangers of seeing the risk management function as the 'No' team

All the case study firms had strong and effective risk management functions, staffed by skilled professionals and capable leaders. Even so, we still observed some of the problems that can be encountered by risk management functions attempting to embed the three modes of accountability across their organisation: problems that are intensified when a risk function is weak or ineffective.

One issue that can prevent the effective working of the three modes of accountability is a lack of value reciprocity (section 3.3.1). If the risk function is unable to convince the wider business that risk management activities add value, then they will not be able to influence these activities in the business units or internal audit. A significant amount of the informal contact the risk managers had with the wider business, including internal audit, was devoted to explaining and demonstrating this value. In particular, we learned that the risk management function must not be viewed as the 'no team':

'…on Monday we had a risk workshop for a new innovation and the project sponsor is the director, unfortunately they actually arrived a few minutes late. And before they arrived, I told everyone in the room that our job here is… It's not the "No" team, it's that we want to encourage innovation, but we want to do it to protect the business and our people, so it's how we do it in the right way.

'And so, when they came in, the first thing they said to our director [was], "well, you're going to say no to this". So, it's changing that attitude that we're not the "No" team, but we're encouraging it to protect people in the business' (Risk Manager).

The risk manager went onto explain that:

'We're evolving, we're changing, we're listening to you so when we start having those connections with those stakeholders their mindset's going to change and they're going to see us more as enablers'.

Interestingly, a business manager confirmed that the risk function in this example were successful in changing mindsets:

'...we always took risks. I think what we've got now... because we've thought about it and we've thought about mitigation and we've thought about the impacts, it's given us more confidence. So while we always took risks as a business, I think what the risk process does is give you more confidence in moving forward and doing them, which obviously then gives you a greater success rate'. ■

When considering the organisation in relation to its inputs and ultimate outputs it is important to understand that its success will be greater than the sum of its components.

'three lines of defence' approach, the risk managers did not talk about this with the wider business. Remaining approachable, to ensure that business managers came to the risk management function with problems or concerns at the earliest opportunity, was viewed as more important than a strict interpretation of the three-lines approach. Other risk managers in the organisation were equally aware of the potential for adverse perceptions:

> *'I think people observe a risk [management] function as this boring admin-driven, task-orientated thing that adds no value to the business'.*
> Risk Manager

Given the pressures of external regulation, the same organisation struggled the most when attempting to influence the risk management activities of the wider business and internal audit. Though most staff were located in one building, we learned that the risk management function was located in a separate area, away from business unit managers. Internal audit was also located separately.

> *'Nobody comes to second line, even the first-line risk and control teams. Nobody comes up there and it's like being summoned to the head teacher's area or something. So there is a bit of a 'them' and 'us' culture that then has materialised again with audit who sit on the third floor, way away from everybody else, which again could be a good thing but…'.*
> Risk Manager

To combat this perception, the risk function used a range of informal mechanisms to reach out to the wider business, notably one-to-one meetings, online chat forums and challenge sessions with senior management. From a complementary formal perspective, the new assessment tool for process risk, though resource intensive to implement, was starting to bear fruit. Several business managers reported that they were using the outputs of the tool to improve the efficiency of their operations:

> *'I think we're at a point now where we question the values of everything to ensure that it's really managing risk, … [the tool is] really helping us understand what the risks are, it's adding value'.*
> Risk Manager

3.4 EMBEDDING RISK MANAGEMENT FOR STRATEGIC SUCCESS

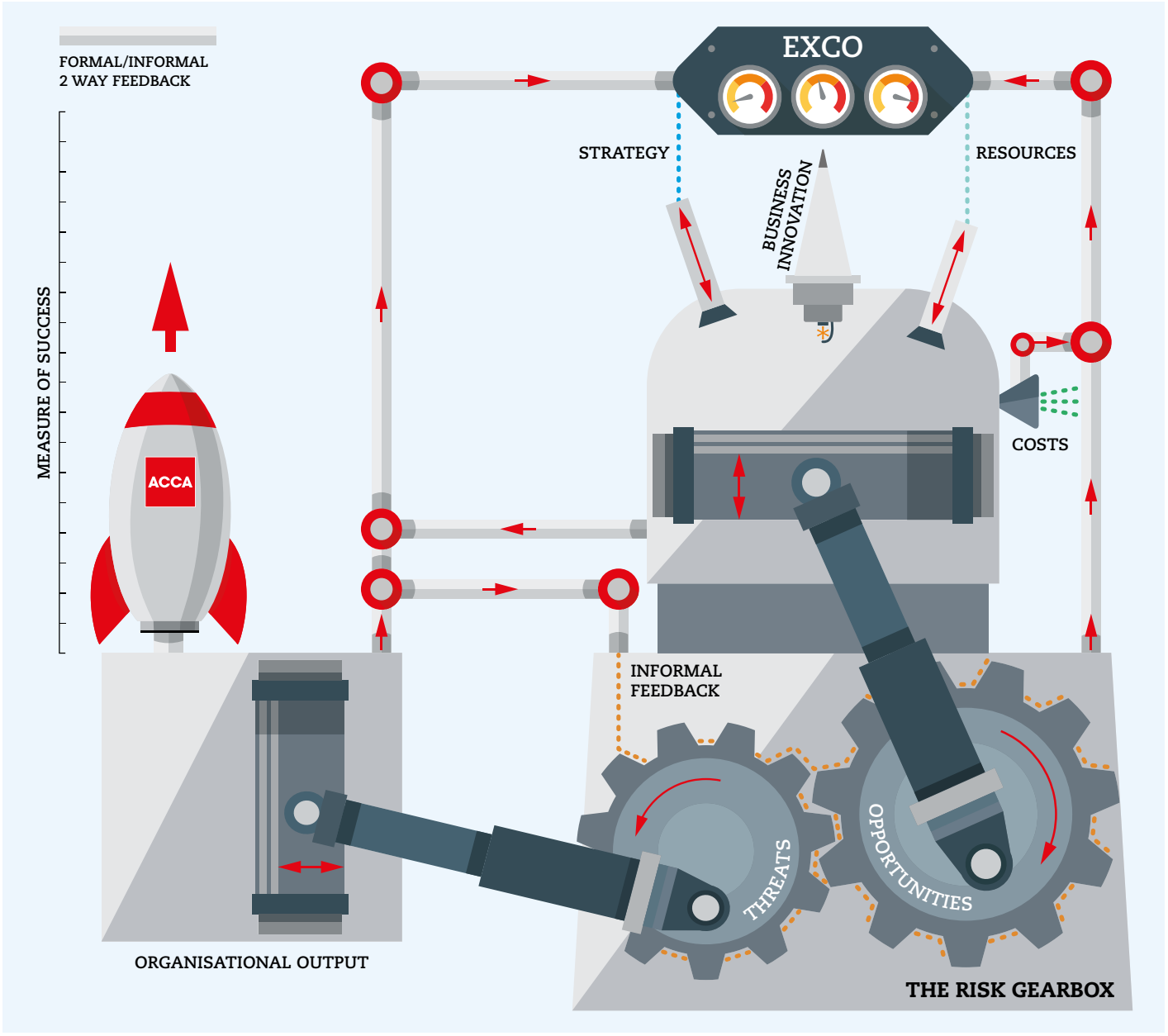
When considering the organisation in relation to its inputs and ultimate outputs it is important to understand that its success will be greater than the sum of its components. We must consider the hierarchical nature of decision making, the multiple processes and layers that assist decision making, and the ability of the organisation to maximise opportunities while minimising threats. Put simply, in the context of our discussion, those organisations that have the ability develop a synergy in their formal and informal risk mechanisms, working in unison across functions and modes of accountability, to address both opportunities and threats, will have an advantage over those competitors who fail to recognise, or worse, fail to act on, those opportunities and threats as they develop.

If we consider the relationship between the various components of the organisation in Figure 3.4, the Executive Committee are central to determining the strategy and resourcing levels of the inputs necessary to achieve business objectives in a cost effective manner. This was evidenced consistently in our earlier publication (Ashby et al. 2018). The potency of the blend of strategy and inputs will also be determined by the spark of business innovation within the organisation as it develops strategic thrust in realising a strategic opportunity by bringing its product/service to the market. Even so, the tone from the top will only penetrate so far, and with the best intentions in the world, it is only when strategic thrust travels down the organisation that the magnitude of potential success will begin to emerge.

An efficient organisational gearbox will enable strategic thrust to become realised opportunities in a way that minimises the effect of threats through the most efficient 'risk gearing ratio' for that organisation.

It is through what we refer to as the 'risk gearbox' that the embedded formal and informal mechanisms of the organisation influence the potency of that strategic thrust. The effectiveness of these formal and informal mechanisms in transferring thrust towards a measurable outcome will be determined by how efficiently the gearbox transforms strategy into a final product/service. An efficient organisational gearbox will enable strategic thrust to become realised opportunities in a way that minimises the effect of threats through the most efficient 'risk gearing ratio' for that organisation (as seen in Figure 3.4). This efficiency will be affected by how coordinated the organisation is in its formal risk mechanisms, how effective its structures of reporting are, and how well supported functions (of which risk management is one of many) understand and facilitate the business in maximising strategic opportunities. This gearing ratio between realised opportunities and threats is not static. In fact, the relationship between the gears is constantly changing as a reflection of the ever-changing competitive marketplace, regulation, and advances in technology experienced by the

FIGURE 3.4: The organisational engine for success



This necessitates the inclusion of 'grease' in the gearbox: that is, the informal mechanisms that ensure that the organisation stays 'risk agile' in the face of change.

organisation – the internal and external factors discussed in section 3.1.3. It is important to note that any one of these developments can create a step change up or down in the output of the gearbox for the organisation. This necessitates the inclusion of 'grease' in the gearbox: that is, the informal mechanisms that ensure that the organisation stays 'risk agile' in the face of change. This ability to make risk-specific decisions in real-time that are supported by formal and informal mechanisms (an efficient 'risk gearbox') maximises the potential for a successful outcome. The momentum of the initial strategic thrust may be lost owing to the imposition of ineffective frameworks, reporting lines, and processes within the organisation (the wrong 'gearing'). At the same time, without supporting informal mechanisms (the right amount of 'grease') the organisation grinds its way through the production process relying solely on sub-optimal formalised mechanisms. Similarly, too much informality/grease and the organisation may lose control of its production process.

The quality of this 'grease' and its effectiveness at lubricating the formalised mechanisms of the organisation will also be determined by the culture of the organisation, and more specifically the perception of the risk function. If the attitudes of the business are that the risk management function is deemed to be the 'no' team, with little or no perception of value-added or trust, then 'value reciprocity' and the advantages it brings will be absent from the 'gearbox'.

Larger organisations, particularly those that are heavily regulated, may take comfort in their formal risk mechanisms. In practice, these may come at the expense of 'value reciprocity' and being 'risk agile', because the risk management function's ability to evidence 'value added' is diluted by the overarching necessity of fiduciary duties and compliance.

As strategic thrust has entered the risk gearbox, fuelled by strategy, resources and innovation, it transforms into a realised opportunity as it leaves for the marketplace. Although this realised opportunity is by no means a guarantee of certain success, it provides reassurance to stakeholders that the organisation has given the innovation the best chance of succeeding in the market. It is at this point that the effectiveness of all the components in the organisational engine can be measured against the success of business outputs. This learning process will itself influence the future behaviour of the organisation through formal mechanisms of information flow and informal 'risk talk'. This is particularly useful should the Executive Committee be quite far removed from the delivery of the final product/service. It provides instant feedback and a basis for the refinement of strategy and resourcing, should it be thought necessary. To return to Figure 3.4, this may affect the future 'gearing ratio' and the extent of 'grease' required. Further, this may differ for any particular organisation – a reflection of the different risk management journeys discussed in section 3.1.3.

In Figure 3.4 the measure of success is currently how high the rocket can fly. With tweaks to the blend of strategy and resources, innovation could be adapted as it passes through the risk gearbox not only to provide upward propulsion to the rocket, but also to increase duration of flight, or possibly by reducing costs allowing the re-use of rockets by landing on floating launch pads, making them more lucrative in the market.

4. Recommendations for practice

This section provides recommendations to improve practice in organisations. These recommendations reflect the practices that we observed in the case studies.

RECOMMENDATION 1: UNDERSTAND FORMAL AND INFORMAL RISK MANAGEMENT MECHANISMS

To embed effective risk management practices in organisations, risk management functions should use a combination of formal and informal risk management mechanisms. The formal mechanisms provide a strong and coherent structure and the informal mechanisms help to ensure acceptance of and engagement in the structure and allow that structure to adapt to changes in the organisation's strategy or risk management objectives.

We recommend that organisations should identify the formal and informal risk management mechanisms that they have and evaluate whether these mechanisms are mutually reinforcing. A cross-disciplinary approach is best, involving the internal audit function, risk management function and HR function and business risk specialists/champions, where relevant. Internal auditors should be involved because of their experience in reviewing and testing a wide range of control mechanisms, HR for its people skills, and risk experts for their knowledge of the formal and informal tools that they are using. We also recommend inputs from business managers, regarding their perceptions of the effectiveness of the formal and informal mechanisms that are in use.

The combined review of formal and informal mechanisms is essential in evaluating the degree of complementarity. The effectiveness of a mechanism on its own is unimportant. What matters is how formal and informal mechanisms complement each other.

A review of formal and informal risk management mechanisms should ask the following questions.

- Is the balance of formal and informal mechanisms appropriate?
- Do formal and informal mechanisms complement each other effectively?
- How can existing formal and informal mechanisms change to improve their complementarity?
- Are additional formal or informal mechanisms required?

RECOMMENDATION 2: RE-THINK RISK GOVERNANCE AS INTEGRATED ACCOUNTABILITY

Rather than organising risk governance in segregated 'lines', we recommend that organisations should adopt an integrated accountability approach. This approach retains the roles of risk taker/controller, risk oversight and risk assurance, but allows greater levels of collaboration and cooperation between the individuals responsible for conducting these roles. This is more reflective of the wide range of circumstances and needs that individual organisations may experience when attempting to embed effective risk management.

Collaboration and cooperation between the business, risk management function and internal audit are essential for embedding risk management in an organisation. Collaboration and cooperation are key informal mechanisms. They mitigate the risk management conundrum by reducing the perceived costs of using formal tools and helping to explain the benefits. Only by working with and getting close to the business units, can a risk management function build

Collaboration and cooperation support the creation of synergies. Staff from business, risk management and audit functions bring different skills, experiences and perspectives to risk management decisions.

trust, and business managers are more likely to engage with it if they accept that the benefits of risk-assessment and control tools outweigh the drawbacks.

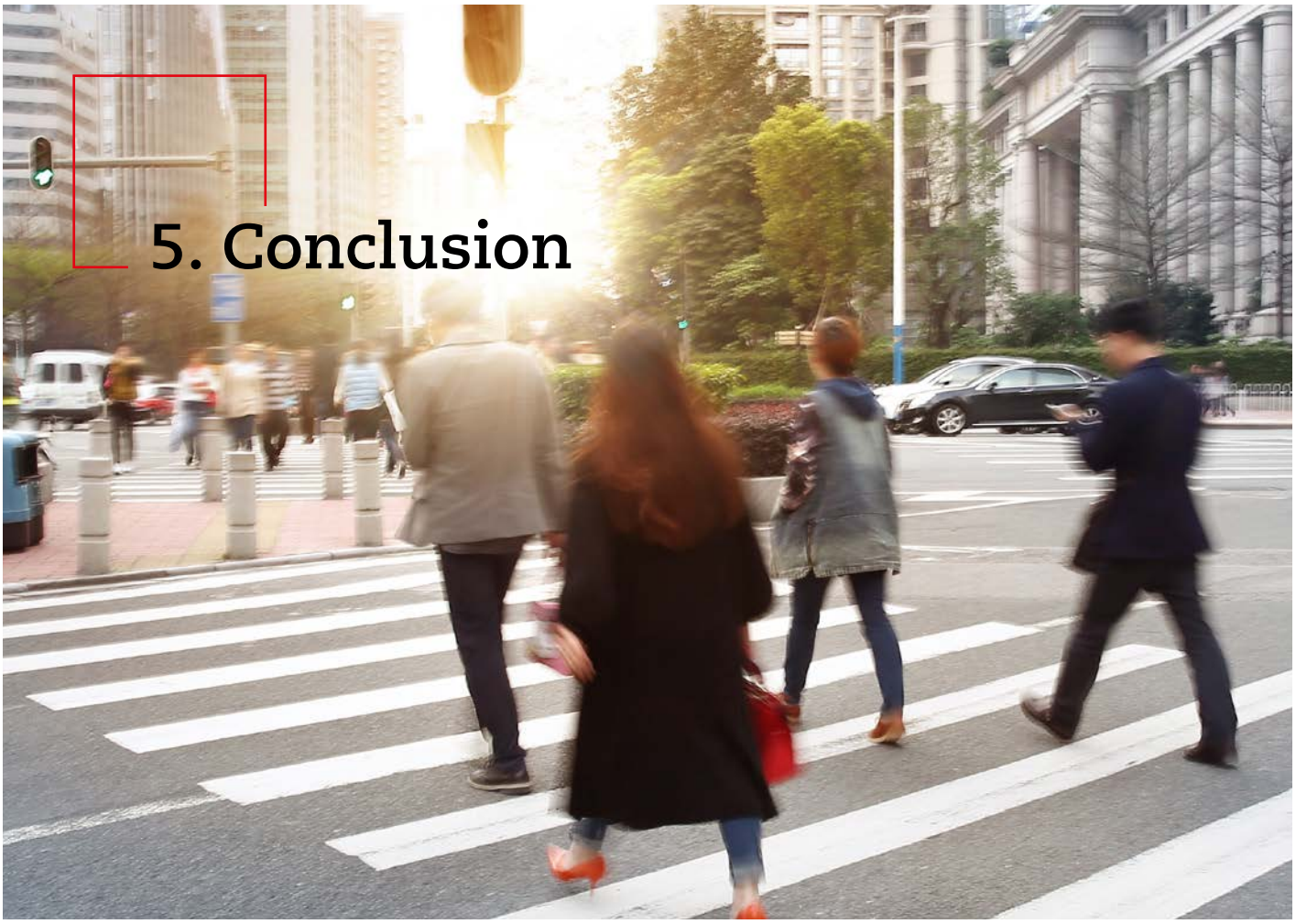
In addition, collaboration and cooperation support the creation of synergies. Staff from business, risk management and audit functions bring different skills, experiences and perspectives to risk management decisions. In section 2.3.1 of our earlier report (Ashby et al. 2018), we showed how boards are most effective when they have 'risk Intelligence', which is a function of their diverse skills, knowledge, education, experience and training (RI-SKEET). A diverse RI-SKEET helps a board to identify, understand, mitigate or exploit a wide range of potential risk scenarios. The same is true of business, risk management and audit staff. More specifically, organisations should look to their risk managers to be relationship builders.

RECOMMENDATION 3: THE TIME AND ATTENTION PUZZLE

It is clear from our research that risk management functions that spend their time administering the risk management strategy of the organisation can become detached from facilitating, and monitoring, the embeddedness of risk management within the business. This leads to a lack of attention to those areas of the organisation where opportunity and threat co-exist, and where the risk management function has the greatest ability to evidence its 'value added'. A failure to seize or maximise those opportunities may reflect the inability of the business to meet the demands of the market; but it may also reflect the risk managers' failure to step away from the spreadsheet and get their hands dirty within the business. It may only be when the risk management function is able to step away from the spreadsheet that the business will begin to understand the value and insight provided and that 'risk management synergy' can develop.

Risk managers should ask themselves the following questions in order to determine whether they are evidencing 'value added' to the business.

- Who ultimately gains from my input and output?
- Do the risk management processes and systems imposed on the business serve me, the business, or both? If not both, why is that? And what can be done to rectify it?
- What proportion of my role is dedicated to maximising opportunities and what proportion is dedicated to minimising threats? Does this balance assist the business in meeting its corporate objectives?



5. Conclusion

There are no easy answers or quick fixes when embedding risk management. What works differs from one organisation to the next. Nevertheless, it is possible to identify common challenges and good practices to overcome these challenges.

The four organisations that we investigated came from different sectors and differed in size, culture and complexity. Each was on a different embedding journey, but they shared very similar risk management objectives. The strategies that they employed to achieve those objectives highlight a range of good practices for any organisation.

Embedding risk management is about much more than formal tool design (eg risk registers, control assessments and risk appetite frameworks). Often the design of a formal tool is less important than the informal mechanisms used to support the tool. Complex tools may not be required. Simple tools, complemented by a broad suite of regular informal mechanisms (one-to-one meetings, etc.) may be more effective than complex tools in embedding risk management. Equally, it is difficult to embed complex tools without significant investment in complementary informal mechanisms.

Developments in risk governance, such as the 'three lines of defence', have not particularly helped embed risk management in the case study organisations. We recognise that this conclusion will challenge some readers and accept that more research is required. Nevertheless, the fact that none of the cases had a pure 'three-lines' approach illustrates the challenges associated with it and the potential value of integrated accountability as an alternative means of approaching risk governance.

We hope that this ACCA Professional Insights report will trigger further debate on embedding risk management in organisations. Just as the organisations studied were on a risk management journey, so is professional practice. Risk professionals and regulators must allow risk management practice to evolve and not divert it into cul-de-sacs based on their own point in time perspective.

Appendix A:
List of interviewees

The table below provides a summary of each case study.

	SECTOR	RISK MANAGEMENT ACTIVITIES	INTERVIEWEE DETAILS
A	Retail financial services (Medium-sized business)	• Multiple divisional and group risk management committees reporting to a board risk management committee. • Second-line risk management function supported by first-line 'risk specialists'. • Implementing a new testing approach to process-risk assessment and control. • Implementing a new IT system for risk data capture, analysis and reporting. • Implementing new risk management reports for committees. • Recently simplified and standardised the risk appetite framework across the organisation.	• Head of risk management function 1 • Second-line business partner • First-line risk specialist (Operations) • First-line risk specialist (finance) • Enterprise risk director • Senior audit manager • HR function head and first-line risk specialist (HR) • Head of risk management function 2 • First-line department head (supply chain)
B	Property development and management (Large business)	• Audit committee chair seen as an effective conduit to the executive committee on matters relating to risk. • The third-line audit and second-line risk function, although independent of each other, are managed collectively and work closely together. • Have developed a fund to allow the first-line business to access resources for risk-related initiatives that are fully financed through insurance policy deductions. • In the process of developing and embedding 'risk champions' in the first line of defence. • Use weekly horizon scans of their industry, and related topics from other industries to communicate risk-related issues to senior managers, group wide.	• Head of internal audit and risk • Risk manager • Communications director • Data protection officer • Risk director • General manager – retail • Central operations director • Group head of security
C	Information technology and financial services (SME)	• Formal risk committee with separate audit committee. • Compliance function separate from risk management function, but close working relationship. • Risk management function supported by risk specialists in key business areas. • Risk management function reports to CFO. • Internal audit carried out by an external provider with additional support from within organisation – up to now overseen by head of risk management. • Have established key risk appetite statements for organisation. Recently implemented new software for capturing and communicating risk control and reporting.	• Risk function business partner (1) • Risk function business partner (2) • Head of risk management • Finance director • Head of compliance • First-line head of department (Customer)
D	Front-line public sector (Very large business)	• Only one formal risk committee the audit and risk committee. At a divisional level, risk management issues discussed during senior management team meetings. • Head of governance leads a risk management function that consists of three teams: risk, assurance and audit relationship management. Internal audit is outsourced. • Second-line risk management function supported by first-line 'risk champions'. • A separate project risk management function exists outside of the head of governance's control. • In the process of implementing a risk appetite framework for the first time. • Risks recorded and reported using risk registers. • Implementing a new risk-assurance approach that will include targeted control testing. • Excel spreadsheets used to collect and store data. Considering purchasing a risk management system.	• Head of governance • Enterprise risk manager • Risk management officer (1) • Risk management officer (2) • Internal audit manager • Programme management team • Head of information and communication technology (ICT) service delivery • Programme risk and communications manager • First-line risk champion (1) • Risk assurance manager • First-line risk champion (2)

To maintain anonymity, we have generalised all interviewee details within the report to one of four general categories ['Board Member', 'Risk Manager', 'Risk Champion', 'Business Manager'] when attributing quotes.

Appendix B:
Supplementary academic literature review

Dr Simon Ashby, University of Plymouth
Dr Cormac Bryce, City, University of London
Dr Patrick Ring, Glasgow Caledonian University

EXECUTIVE SUMMARY

Organisations in every sector, whether large or small, simple or complex, invest time and resources in managing risk. Effective risk management is an essential element in the success or failure of these organisations, but there remains much to learn about what 'effective' means. ACCA's report on board level risk management practices, *Risk and the strategic role of leadership* (Ashby et al. 2018), highlighted the significance of risk in the boardroom and how boards organise their risk management activities to inform strategy and governance. In the report published alongside this literature review, we investigate how board-level risk-taking and control objectives translate into the risk management activities performed within organisations. The aim is to understand how these activities are embedded to ensure that staff across the organisation collaborate and cooperate to manage risk in a manner that is consistent with the board's risk-taking and control objectives. Effective risk management within organisations can only be achieved when staff are willing to engage in relevant activities to achieve the board's objectives. In short, risk management cannot be effective if it is not embedded.

The project is based on:

- four in-depth case studies, which included documentation reviews, site visits and 34 interviews across a range of business functions
- two focus groups consisting of a number of risk management professionals, and
- input from the ACCA's Global Forums, with particular thanks to the Global Forum on Governance, Risk and Performance.

The research shows that although the case study organisations had similar risk management objectives, the paths they took to embedding risk management varied according to the external environment in which they operated and a range of internal factors, such as leadership tone and the success or failure of past risk management initiatives. Organisational paths varied in the risk management mechanisms that they used and, in particular, the formality or informality of these mechanisms.

Key findings include the following.

- Effective risk management requires the use of complementary formal and informal mechanisms. Formal mechanisms include risk registers, control assessments, internal audits and risk reports. Informal mechanisms include social networking and sales/influencing techniques.
- Communication is vital. This includes communication between business units and functions, as well as communication to/from the risk management function and internal audit function.
- The risk management function has a pivotal role in communication and building risk management relationships. This function operates as a nexus for risk management communication, facilitating communication between business units and functions and to/from the internal audit function and board/senior management. A risk management function that cannot build effective relationships across an organisation will not be able to embed effective risk management.
- The risk management function does not only design and implement risk identification, assessment and reporting tools, it must also work hard to explain and even sell the benefits of risk management to the wider organisation.
- Every case study organisation struggled with the requirements of a pure 'three lines of defence' model for risk governance. We propose reformulating the three lines model to create a less segregated, 'modes of accountability' approach.

Within the report we consolidate our findings into a conceptual model for embedding risk management in organisations. We call this the 'risk gearbox' and show how formal and informal risk management mechanisms combine to create 'strategic thrust' to support the strategic risk-taking and control decisions of the board. We also provide a number of recommendations for organisations looking to improve the effectiveness of their risk management arrangements.

SUPPLEMENTARY MATERIAL: PRIOR RESEARCH ON EMBEDDING RISK MANAGEMENT

The academic literature on implementing and embedding risk management activities has grown since the financial crisis. This research is case-study based, exploring the 'black box' of risk management practice within organisations. In-depth case studies are required to explore how formal risk management tools and techniques influence and are influenced by the people who use them. For the interested reader, we provide below a brief analysis of the academic literature that complements the main report.

FORMAL AND INFORMAL ORGANISATION

A central theme in the literature is the interplay of formal and informal organisation. A two-case study paper on the subject (Arena et al. 2017) conceptualises enterprise risk management (ERM) as a mix of formal and informal 'boundary objects', including: tools (eg risk matrices), processes (risk identification and categorisation) and governance networks that coordinate and communicate knowledge about risk. Boundary objects are formal or informal devices that help the individuals within a social group to collaborate and coordinate their activities and together these objects combine to form a boundary infrastructure. Arena et al. (2017) explain that organisations may design their boundary infrastructures in a variety of ways, to meet diverse management objectives (eg internal control versus entrepreneurial activity), but that these infrastructures often have weaknesses that make them unstable and reflect the tensions that exist between the formal and informal modes of organisation. The weaknesses identified in the two case studies highlight a tension between the 'robust' and 'plastic' nature of boundary objectives (having something that is consistent versus something flexible). In one case, the weakness is that the ERM approach is too procedural and control oriented, emphasising the robust nature of a boundary infrastructure at the expense of plasticity. As a result, the organisation's ERM approach did not meet the diverse needs of management. In the other case study, the ERM approach was much less formal and supported management decision making better (the plastic nature of the boundary infrastructure dominated robustness), but did not provide adequate assurance on internal control.

In contrast to Arena et al. (2017), Kaplan and Mikes (2016) combine previous case study research to examine how organisations can mitigate the instability of their boundary infrastructures to balance the formal (more robust) and informal (more plastic) objects that constitute these infrastructures. The roles of the risk function and chief risk officer (CRO) are key, as well as how they support creativity and innovation while at the same time ensuring appropriate control over excessive (or insufficient) risk taking. Central to this role is the ability of a CRO/risk management function to facilitate 'risk talk', which is a form of conversation that is based on deliberate, analytical and evidence-based thinking (known as 'system 2 thinking'), rather than emotion or instinct ('system 1 thinking'). Effective risk talk is forward looking and designed to help organisations identify, assess and control opportunities and threats at the earliest opportunity.

Kaplan and Mikes distinguish between the following roles for the CRO/risk function:

- independent overseers
- business partners
- independent facilitators, and
- dual or hybrid function, combining the overseer and partner types.

Independent-overseer risk functions emphasise risk oversight and the formal segregation of the first, second and third lines of defence. These functions maintain independence, but their distance from the wider business can prevent them from obtaining a complete picture of the organisation's risk profile, especially when a lack of personal contact with business managers results in low levels of trust.

CROs/risk functions that adopt a 'business partner' role are less formal in their interpretation of the three lines and emphasise closeness with business management, helping to build trust and improving communication and reporting. But this closeness may affect the independence of the risk management function and lead to less effective oversight and challenge.

Dual or hybrid functions attempt to combine the overseer and partner roles, with varying degrees of success, and independent facilitators represent the ideal type of CRO/risk management function for Kaplan and Mikes. Independent facilitator CROs/functions combine a strong technical ability in risk management with excellent interpersonal and communication skills, facilitating effective risk talk. They operate in a manner similar to an external consultant, providing advice, guidance and challenge where necessary.

EMBEDDING AS A JOURNEY TO A DESTINATION THAT IS NEVER QUITE REACHED

Embedding is a long-term exercise to place (and keep) risk at the heart of an organisation's decision-making processes. Embedding is effective when: 'the ERM agenda becomes central to managerial decision making', as opposed a situation where risk management 'appears to occupy a purely ritualistic role of impression management' (Jordan et al. 2013: 157). Embedding is the solution to a common governance problem. As organisations grow and diversify it is difficult for the board and executive to control the management of risk (whether in mitigating threats or exploiting opportunities). Though boards retain ultimate responsibility for an organisation's risk management agenda, day-to-day management must be delegated, but how can the board/executive ensure that delegated decisions and activities are consistent with their agenda? (Fraser and Henry 2007). Embedding may also be inherently unstable (Arena et al. 2017), driven by the tensions between risk as an opportunity and threat, and reflected in the tensions between the plastic and robust characteristics of ERM boundary infrastructures. Opportunity exploitation requires plasticity, threat avoidance, robustness.

The fact that the design of ERM boundary structures will affect their implementation and vice versa creates a second embedding challenge. These feedback loops may be positive or negative. Good implementation can lead to a more effective design and a more effective design may support its successful implementation (Arena et al. 2011). But there can be instabilities, again linked to the problem of balancing potentially conflicting risk-taking and control objectives (Arena et al. 2017).

In a German case study, Tekathen and Dechow (2013) investigate the implementation of an ERM boundary infrastructure. They report that the infrastructure does intensify business-level focus on and discussions about risk. But differences in local practices in using ERM make aggregation and cross-function discussions about risk much more difficult. Each local area in their study adapted the infrastructure to meet its own needs and struggled to think outside the local context. Hence, a common ERM infrastructure does not guarantee coordination and effective communication across the organisation.

Jordan et al. (2013) provide a good example of the relationship between the design of a risk management tool (a risk matrix and risk-reporting map based on the matrix) and its implementation in a single case study analysis (see also Jordan et al. 2018). Jordan et al. (2013) allege that risk matrices/maps can be a symptom of disengaged and weakly embedded risk management; this can occur where formal tick-box-style processes and documents are used to protect an organisation from 'secondary' risks related to a loss in reputation or to compliance concerns. The purpose of secondary risk management is to avoid blame for alleged mismanagement and protect against fines, bad press, litigation or similar. Jordon et al.'s case study (2013) shows that risk maps can be used to evidence commitment (to managing a project and its associated risks, for example), facilitate coordination and support conversations about risk and the achievement of project objectives. Jordan et al. (2013) conclude that risk management tools per se are not the problem, but how the tool is used can be. Even formal tools can support risk talk and effective decision making, while providing a mechanism for managing responsibility and accountability (blending the robust and plastic nature of a boundary object and associated infrastructure).

Woods (2007) shows how non-risk management tools may be integrated with ERM boundary infrastructures to enhance their implementation. Woods uses a single case study of Tesco Plc to show how risk and strategy may be integrated using a balanced scorecard performance-management tool. The Tesco approach enables all staff to think about risk and understand how their actions may support strategic objectives. It also ensures that decision making is coordinated and contained (within risk appetite) and provides information to the board/senior management. The use of the ERM integrated balanced scorecard is supported by clear accountabilities, top-down and bottom-up communication and an internal audit function that works as an independent facilitator. Woods (2007) notes that the approach may not work for high-risk sectors such as financial services, given the low profile of risk assessment of reporting and a lack of formal risk management language. Risk is so well embedded into Tesco's performance-management system that it is not always thought about as risk.

TOOL MAKING BY THE RISK FUNCTION

Meidell and Kaarbøe (2017) use a longitudinal (18-year) case study of an oil company to investigate how a risk management function can use risk management tools (risk registers, reports, etc.) to influence decision making. Meidell and Kaarbøe adopt a sense-giving perspective to explore how a risk function can influence the sense-making of others in the organisation (ie how people across the organisation understand risk and engage in their employer's risk taking and control objectives). They show that the power of risk management sense-giving is affected by tool design and how the risk function uses its specialist knowledge to support knowledge sharing and collaboration across the various socio-cultural boundaries of a business (ie between business units and functions) to influence decision making. Using the case study, they show how various tools designed and or supported by the risk function (eg risk maps) increased the influence of the function over decision making across the organisation. But they found that tools are not sufficient on their own to support sense-giving. Also key is the ability of the risk management function to 'sell' the tool to group senior management and to provide support to the middle-managers across the organisation's business units and functions on how to use and interpret the output from the tools (which Meidell and Kaarbøe term 'managing the knowledge boundary').

Hall et al. (2015) provide two longitudinal case studies of risk management toolmaking and use in UK banks. Like Meidell and Kaarbøe (2017) they find that the influence of the risk function can be affected (for better or worse) by the design and implementation of risk tools. In one case study, the risk management function relied on the expertise and social networks of some long-standing risk managers, but this function lost traction as the old guard retired and were replaced by new, more compliance-focused risk managers. These new risk managers developed tools that satisfied regulatory requirements rather than business need. In the other case, the risk management function developed and adjusted tools to suit the needs of the business. As a result, risk managers maintained high levels of influence, including influence over strategic decisions. Using the case studies, Hall et al. (2015) identify two types of risk management toolmakers: compliance experts (focused on regulation) and engaged toolmakers (focused on business need). They conclude that to gain traction, tools must be unique (not available elsewhere) and relevant (to the business), and must support effective communication/coordination and decision making. In this respect simpler, less quantitative tools can have an advantage, as they are easier to understand and adaptable to business needs. Nonetheless, for the risk management function to retain influence, tools should not be so simple that the function's expert input is no longer required. If the risk management function can get the balance right, then tools can be used to enhance the function's

credibility. Good tools, perceived as having value in the wider business, can increase the level of trust in the function and its ability to influence decision making.

Palermo (2014) argues that a risk function can, though toolmaking, offer solutions that meet external (institutional) and internal (managerial) needs. Palermo demonstrates this using a single case study of a UK public sector organisation. Like Hall et al. (2015), Palermo finds that the key to success is the business experience and soft skills of the risk management function and local-level risk champions, rather than technical risk management knowledge. This lends support to the argument that risk experts may be especially effective when they work as independent facilitators and risk communicators. Palermo also demonstrates the value of business unit or functional-level risk champions in supporting the work of the risk management function and embedding risk management.

NO 'ONE SIZE FITS ALL': A CONTINGENCY THEORY OF EMBEDDING RISK MANAGEMENT

Though the structure of risk management activities (identify, assess, control, monitor and report) may be similar (Woods 2007) the tools that are used and how these tools are implemented (the content of the structure) are contingent on organisation-specific factors such as size, governance structures, technology and regulation. The factors that influence the design and implementation of risk management tools form what is known as the 'contingency theory of risk management' (Mikes and Kaplan 2015; Collier and Woods 2011; Woods 2007.

From a contingency theory perspective, a variety of tools and implementation approaches can embed risk management in organisations (Fraser and Henry 2007; Kaplan and Mikes 2016; Mikes and Kaplan 2015; Schiller and Prpich, 2014). These embedding strategies reflect different blends of formal and informal approaches to tool design and implementation (Arena et al. 2011; Arena et al. 2017; Schiller and Prpich 2014). Formal approaches are prescriptive and standardised, with an emphasis on consistent decision making and limiting discretion. Informal approaches are more business oriented and flexible, with an emphasis on simple tools and connecting people and problems via 'risk talk' (social interaction).

Though there may be no best approach to tool design and implementation, there is greater consensus on the use of risk management. The weakest approach uses risk management for compliance and control of downside risk only (an emphasis on value protection). A stronger approach promotes appropriate risk taking and uses risk management to support strategic decisions (risk management is used for value creation).

Within this value protection and creation spectrum, Arena et al. (2011) identify three common approaches:

- responsive – the weakest approach, it is backward looking, reactive and focuses on compliance and reputation protection
- discursive – a mid-range approach, emphasises current risk exposures and focuses on knowledge sharing to coordinate risk management activities and ensure consistent decision making, and
- prospective – the strongest approach, forward looking and considers the relationship between strategy and risk.

A TENTATIVE CONCLUSION

Case study research looks deep into a small number of organisations. Nonetheless, as the number of in-depth cases grow, conclusions on how to embed risk management are emerging. These conclusions are consistent with our findings and the recommendations in section 4 of the main report.

1. To be embedded, risk management activities must be forward looking to meet the needs of the organisation and its stakeholders.
2. Risk management activities must accommodate a diverse range of stakeholder needs, including threat reduction and the exploitation of future business opportunities.
3. Key business needs include effective communication and strategic/tactical decision making. Risk management activities must support both.
4. Risk management activities best support communication and decision making when they combine formal and informal mechanisms. From an informal perspective an essential element is 'risk talk'.
5. Risk management activities should be supported by a risk management function that designs organisation-appropriate risk identification, assessment, reporting and control tools and helps decision makers to use these tools. The appointment of local risk champions and a CRO will support the work of the risk function.
6. The effective use of risk management tools is reinforced by complementary governance and performance-management arrangements.

References

Arena, M., Arnaboldi, M. and Azzone, G. (2011), Is Enterprise Risk Management Real? *Journal of Risk Research*, 14 (7): 779–97.

Arena, M., Arnaboldi, M. and Palermo, T. (2017), 'The Dynamics of (Dis) Integrated Risk Management: A Comparative Field Study', *Accounting, Organizations and Society,* 62: 65–81.

Ashby, S., Bryce, C. and Ring, P. (2018) *Risk and performance: Risk and the strategic role of leadership,* ACCA Professional Insights Report <https://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/Risk-and-the-strategic-role-of-leadership/pi-risk-strategic-leadership.pdf>, accessed 29 March 2019.

Collier, P.M. and Woods, M. (2011), A Comparison of the Local Authority Adoption of Risk Management in England and Australia. *Australian Accounting Review*, 21 (2): 111–23.

Fraser, I. and Henry, W. (2007), 'Embedding Risk Management: Structures and Approaches', *Managerial Auditing Journal,* 22 (4): 392–409.

Hall, M., Mikes, A. and Millo, Y. (2015), 'How Do Risk Managers Become Influential? A Field Study of Toolmaking and Expertise in Two Financial Institutions', *Management Accounting Research*, 26 (1): 3–22.

IRM (Institute of Risk Management) (2012) *Risk Culture under the Microscope: Guidance for Boards* (London: IRM).

Jordan, S., Jørgensen, L. and Mitterhofer, H. (2013), 'Performing Risk and the Project: Risk Maps as Mediating Instruments', *Management Accounting Research,* 24 (2): 156–74.

Jordan, S., Mitterhofer, H. and Jørgensen, L. (2018), 'The Interdiscursive Appeal of Risk Matrices: Collective Symbols, Flexibility Normalism and the Interplay of "Risk" and "Uncertainty"', *Accounting, Organizations and Society*, 67 (5): 34–55.

Kaplan, R.S. and Mikes, A. (2016), 'Risk Management – The Revealing Hand', *Journal of Applied Corporate Finance*, 28 (1): 8–18.

Meidell, A. and Kaarbøe, K. (2017), 'How the Enterprise Risk Management Function Influences Decision-Making in the Organization – A Field Study of a Large, Global Oil and Gas Company', *The British Accounting Review,* 49 (1): 39–55.

Mikes, A. and Kaplan, R.S. (2015), 'When One Size Doesn't Fit All: Evolving Directions in the Research and Practice of Enterprise Risk Management', *Journal of Applied Corporate Finance*, 27 (1): 37–40.

Palermo, T. (2014), 'Accountability and Expertise in Public Sector Risk Management: A Case Study', *Financial Accountability & Management*, 30 (3): 322–41.

Schiller, F. and Prpich, G. (2014), 'Learning to Organise Risk Management In Organisations: What Future for Enterprise Risk Management?', *Journal of Risk Research*, 17 (8): 999–1017.

Tekathen, M. and Dechow, N. (2013), Enterprise Risk Management and Continuous Re-Alignment in the Pursuit of Accountability: A German Case', *Management Accounting Research*, 24 (2): 100–21.

Woods, M. (2007), 'Linking Risk Management to Strategic Controls: A Case Study of Tesco plc', *International Journal of Risk Assessment and Management*, 7 (8): 1074–88.

PI-EMBEDDING-RISK-MANAGEMENT

ACCA The Adelphi 1/11 John Adam Street London WC2N 6AU United Kingdom / +44 (0)20 7059 5000 / www.accaglobal.com